AGENCY OF HUMAN SERVICES

AHS System Acquisition Guidelines

Jack Green

10/23/2013

The purpose of this guideline is to facilitate the implementation of the Vermont Health Connect's security control requirements for the System Acquisitions (SA-2, SA-4(1) Controls.

Revision History

Date	Version	Description	Author
	1.0	Created many of these clauses	Darin Prail/Frank Cresenzi
5/2/2013	2.0	Created document and piloted implementation	Jack Green
10/24/2013	3.	Document revised for AHS standards, added clauses	Jack Green

PURPOSE/STANDARD STATEMENT:

The purpose of this guideline is to facilitate the implementation of the Vermont Agency of Human Services security control requirements for the System Acquisition (SA-2, SA-4(1) Controls.

The information systems covered in this guideline document contain but are not limited to the following:

- Programming Projects hosted internally
- Externally Developed Applications
- Externally Hosted Applications
- Software Provided as a Service
- IT Projects in general

SCOPE

The scope of this guideline includes the AHS

STANDARD

The following security-based items should be considered when crafting an RFP or a contract. A clause corollary to the abstract items is listed in the table. These clauses may be pasted into the RFP/Contract document.

ABSTRACT

The following table describes in detail the policies described by AHS and by DII with respect to security policy and Data Standards. Once approved this document must be included in all IT-based RFP's and contracts. The bulleted list below is the essence of the document.

- The State owns its data
- Data must be made available on request, delivered appropriately
- State has 6 months to transfer its data before contractor can delete
- Contractor surrenders data before going out of business (tough to enforce)
- The contractor agree to report a security breach and notify victims
- The AHS security event definition
- Log and save security events for 1 year
- Confidentially agreements may be required
- Hosting must be done in the US

- The State may audit infrastructure
- State may run network audits or port scans.
- Contractor must run quarterly pen tests, report results as a deliverable
- Contractor should adhere to basic application security practices.
- All PII Data must be encrypted
- The State data owner may ask that other sensitive data be encrypted.
- Backups must occur at regular intervals
- Encryption of PII must not impact program functionality
- Encryption must use cryptographic key hierarchy
- The minimum encryption level is AES 128
- The AHS standard data element definition and code template must be used and is a deliverable.
- Communications with the State are public property and subject to statutory restrictions
- Sharing of information is based upon HIPAA need to know
- Use (TLS) secure email for PHI/PII
- The Contractor must describe the functional properties of its security controls

CLAUSES

HOSTING, OWNERSHIP OF DATA, DATA PORTABILITY	
State's Ownership of Data and Portability Following Contract Termination The State's information, or any derivatives thereof, contained in any Contractor-owned repository (the "State Data," which shall also be known and treated by Contractor as Confidential Information) shall be and remain the sole and exclusive property of the State. The State shall be entitled to an export of State Data, without charge, upon the request of the State and upon termination of this Agreement. Following contract termination, the State will retain ownership of all database information, including specific client-level data and aggregate data sets.	The State owns its data
The Contractor agrees to deliver all data to the State upon the State's request, and the Contractor will possess no lien or other such rights to the data. Data transfer, storage, and retrieval Guidelines must protect the original data from alteration. The data shall be delivered in a standard, agreed-upon format by the Contractor for the full range of customer data and will be transmitted to the State through secure means. Data will include a data dictionary as defined in requirements listed under the section ***Data Dictionary***	Data available on request, delivered appropriately
After the termination of this contract the State will have up to six (6) months of full access to State data (client-level data and aggregate data sets) to obtain downloads of all data to a container within the Vermont Agency of Human Services system or another hosted solution before the Contractor can destroy client-level data and aggregate data sets. Once the State has acknowledged in writing to the Contractor's legally appointed representative that all data have been downloaded, the Contractor will destroy all State data and supply the State with a certified affidavit that all data, including backups, have been destroyed in accordance with privacy and security standards	State has 6 months to transfer its data before contractor can delete
In the event that the Contractor goes out of business before the end of this agreement, the Contractor agrees to deliver all data to the State upon the State's request, and the Contractor will possess no lien or other such rights to the data. Data transfer, storage, and retrieval Guidelines must protect the original data from alteration. The data shall be delivered in a standard, agreed-upon format by the Contractor for the full range of customer data and will be transmitted to the State through secure means. Data will include a data dictionary as defined in requirement 10.13.1. The Contractor will ensure that data is not available to any other entities but the State.	Contractor surrenders data before going out of business (tough to enforce)
The Contractor, within one day of discovery, shall report to the State any security breach. The Contractor's report shall identify: (i) the nature of the security breach, (ii) the State Data used or disclosed, (iii) who made the unauthorized use or received the	Agree to report a security breach and notify victims

unauthorized disclosure, (iv) what the Contractor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action the Contractor has taken or shall take to prevent future similar unauthorized use or disclosure. The Contractor shall provide such other information, including a written report, as reasonably requested by the State. The Contractor agrees to comply with all applicable laws that require the notification of individuals in the event of unauthorized release of personally-identifiable information, including, but not limited to Chapter 62 of Title 9 of the Vermont Statutes or other event requiring notification. In the event of a breach of any of the Contractor's security obligations or other event requiring notification under applicable law ("Notification Event"), the Contractor agrees to assume responsibility for informing all such individuals in accordance with applicable law.	
Security events will be reported to the State. Security-related events include, but are not limited to: □ Evidence of unauthorized access to privileged accounts □ Evidence of unauthorized access to data.	Security event definition
All security-related events on critical or sensitive systems must be logged and audit trails saved for one year.	Log and save security events for 1 year
Hosting and Security Standards If the State determines it is needed, the Contractor will sign a confidentiality agreement.	Confidentially agreements may be required
The contractor must host the State's solution within the United States of America.	Hosting done in the US
The State reserves the right to periodically audit the contractor application infrastructure to ensure physical and network infrastructure meets the configuration and security standards and is in adherence to relevant state policies governing the system.	State may audit infrastructure
The State reserves the right to run non-intrusive network audits (basic port scans, etc.) after providing 24 hour notice of the date and time of such scans. More intrusive network and physical audits may be conducted on or off site with 24 hours' notice.	State may run network audits or port scans.
The Contractor will have a third party perform methodology-based (such as OSSTM) penetration testing quarterly and be willing to provide results of that testing to the State.	Contractor must run quarterly pen tests
The Contractor will review the application and certify it meets the	Contractor should

following: - Identify the key risks to the important assets and functions provided by the application and conduct an analysis of the Top 25 software errors (http://cwe.mitre.org/top25), or most common programming errors, and document in writing that they have been mitigated. - Ensure all application code and any new development meets or exceeds the OWASP Application Development Security Standards outlined on the www.OWASP.org site (currently https://www.owasp.org/images/4/4e/OWASP_ASVS_2009_Web_App_Std_Release.pdf) and document in writing that they have been met.	adhere to basic application security practices.
The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls. (NIST 800	The Contractor must describe the functional properties of its security controls
Data Base Standards	
All personally identifiable information (PII) data must be encrypted, to include data at rest and data in motion, particularly when the State is not in physical control of the data.	All PII Data must be encrypted
Additional program data, as determined by the data owner, may also be encrypted.	The State data owner may ask other data to be encrypted.
1. Full daily backups must be taken unless the database is very large, then full weekly backups and daily differential backups must be taken.	Backups must occur at regular intervals

2. Full daily backups must be taken unless the database is very large, then full weekly backups and daily differential backups must be taken. 3. Database backup files must not be stored on the same subsystem as the primary database files. Separate storage is necessary. a.	
Data encryption methods may encompass cell-level, table-level, database-level, or file-level encryption, as long as PII and data owner specified control requirements a are met. Additionally, all applications, APIs, and services must be able to consume the data successfully using the selected method(s) of encryption.	Encryption of PII must not impact program functionality
Encryption must use cryptographic key hierarchy conventions or its equivalent	Encryption must use cryptographic key hierarchy
For encryption level, no encryption and simple encryption are unacceptable. 3DES encryption is acceptable as long as the data resides within the State network at all times. AES encryption with keys of at least 128 bit blocks is preferred.	The minimum encryption level is AES 128
Data Dictionary - http://confluence.ahs.state.vt.us/display/AHSDS/Data+Dictionary+Template	A data element definition and code template.
Contractor Communications with State Employees	
http://humanservices.vermont.gov/policy-legislation/policies/05-information-technology-and-electronic-communications-policies/5-01-email-use/view	Communications with the State are Public Property and subject to Statutory Restrictions
http://humanservices.vermont.gov/policy-legislation/policies/05-information-technology-and-electronic-communications-policies/5-03-access-control/view	Sharing of information is based upon HIPAA need to know
Whenever PII/PHI information are emailed, them email must be encrypted in transit	Use (TLS) secure email for PHI/PII
End of Document	

IMPORTANT INFORMATION

These Guidelines can be found at http://dvha-intra.ahs.state.vt.us/policies-protocols/InfoSec